Security in the Future Computing Environment

David B. Nelson, Ph.D., CISSP

Director

National Coordination Office for

Information Technology Research and Development

May 14, 2003

IT Security and Assurance Conference and Exposition

Huntsville, AL

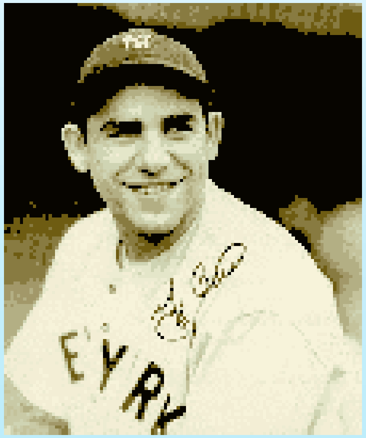
Security Concerns Are Evolving

- **Classic security concerns deal more with data**
  - Confidentiality (data only available to those authorized)
  - Availability (you can get it when you want it)
  - Integrity (data hasn't been changed)
- **Additional concerns deal more with people and transactions**
  - Trust (Who you are and what you are authorized to do)
  - Non-repudiation (You can't deny doing something you did)
  - Auditability (I can check what you did to the data)
  - Reliability (The system does what I want when I want it to)
  - Privacy (Within certain limits no one should know who I am or what I do)

Looking Ahead Helps Us Prepare, However ...

“Predicting is tricky, especially about the future”

–Yogi Berra



Likely Characteristics of Future Computing Environment (1)

- **Critical to the enterprise**
  - Agent for most business
  - More robust and self-regulating (autonomic computing)
- **Widely distributed**
  - “The network is the computer” - Scott McNealy
  - Use of middleware: Grid services, Web services, collaboration tools
  - Computing on demand using remote resources
- **Ubiquitous**
  - Always available by wireless and wired connections
  - Portable identity and workspace
  - Human-centric with improved collaboration, communication, and resource discovery tools
- **Heterogeneous**
  - Many different kinds of devices with different power and characteristics
  - Alternative technologies for organization/presentation of data

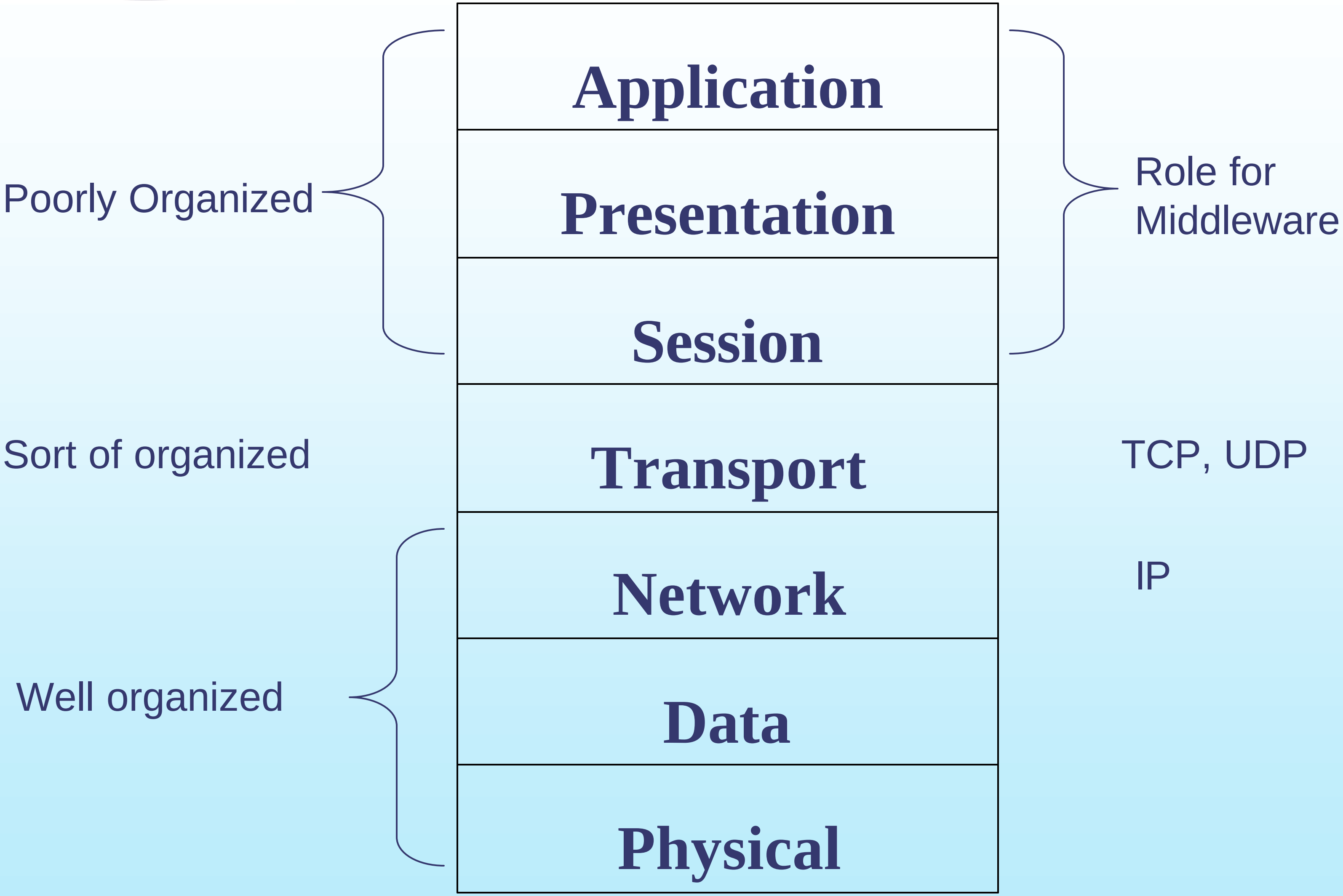
Likely Characteristics of Future Computing Environment (2)

- **Extended beyond organizational boundaries**
  - Virtual organizations
  - Membership and trust issues
- **Dynamic**
  - Discovery and use of resources
  - Management and configuration issues
- **Mediated by middleware**
- **Challenging to maintain security**
  - Hard to determine what is inside vs. outside
  - Hard to determine appropriate usage/users for identity, authentication, authorization
  - Web Services will mean port 80 is used for "everything"
  - Increasing demands for privacy and anonymity
  - Need for role-based security
- **If we are very lucky, perhaps re-designed to be more intrinsically secure**

Challenges of Future Computing Environment to Security Community

- How to accommodate vision of large-scale collaborations, access to resources, eCommerce, without compromising security?
- How to accommodate changing environment within current framework of risk management?
- How to evolve security practices and technologies to keep up with future computing environment?
- How to build security into architecture of future environment, including ability to withstand, identify, and respond to attacks?
- How to say “yes” rather than “no” to users and developers while not compromising security?

Middleware Is Software That Helps Organize ISO Network Layers 5-7



Poorly Organized	Application	Role for Middleware
	Presentation	
	Session	
Sort of organized	Transport	TCP, UDP
Well organized	Network	IP
	Data	
	Physical	

ISO 7-layer Network Model

Grid Computing: Example of Distributed Computing Enabled by Middleware

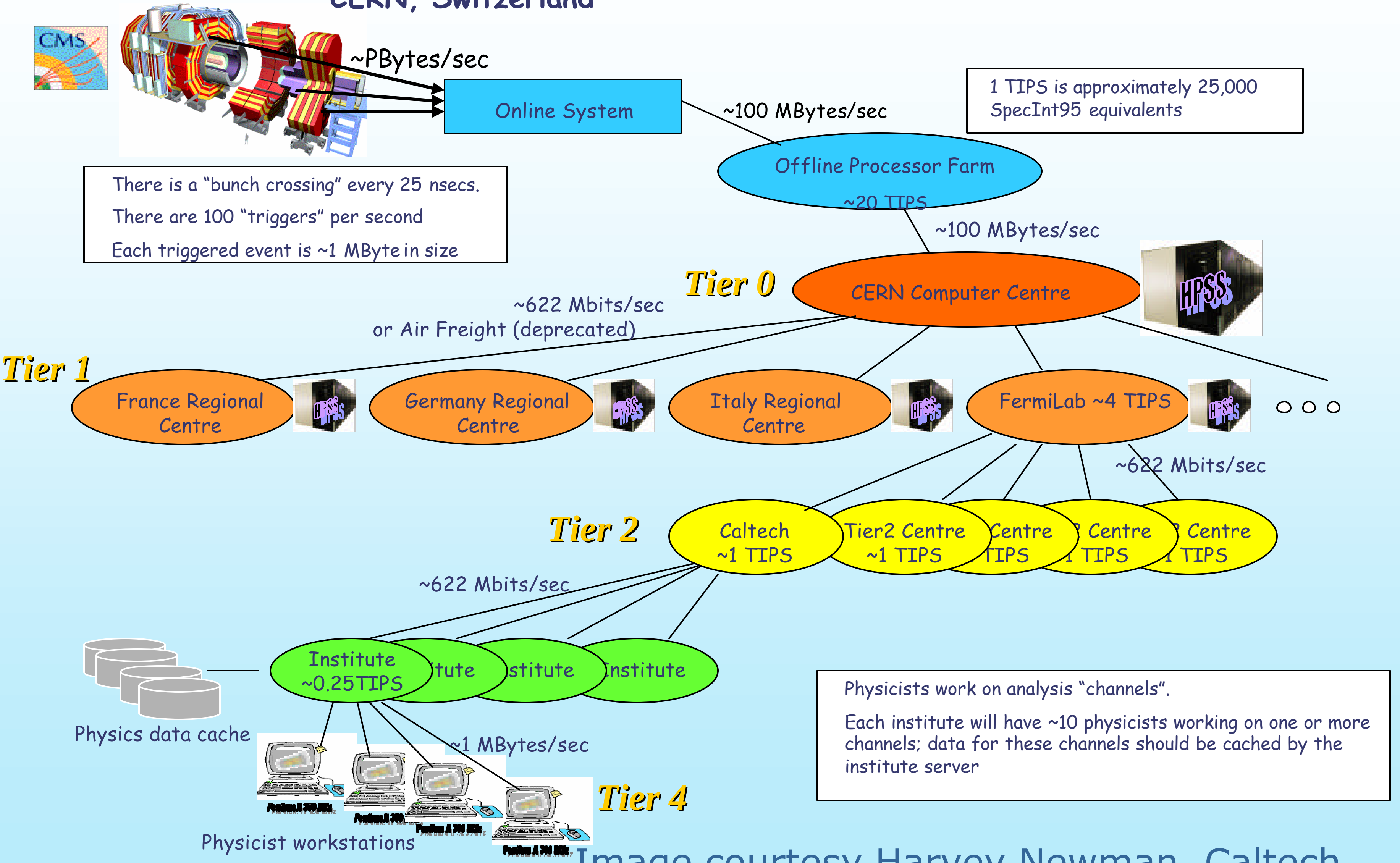
- **Goal: Enable a geographically distributed community [of thousands] to perform sophisticated, computationally intensive analyses on Petabytes (10^{15} bytes) of data**
- **Organizations coordinating Grid tools and security**
  - Global Grid Forum www.ggf.org
  - Globus Project www.globus.org
- **Standards: Open Grid Services Architecture, Open Grid Services Infrastructure (uses Web services)**
- **Globus Toolkit™ centers around four key protocols**
  - *Security*: Grid Security Infrastructure
  - *Resource Management*: Grid Resource Allocation Management
  - *Information Services*: Grid Resource Information Protocol
  - *Data Transfer*: Grid File Transfer Protocol (GridFTP)

Examples of Data Grid Projects

- **European Data Grid (EU)**
  - DG technologies & deployment in EU
- **GriPhyN (NSF)**
  - High Energy Physics, Investigation of “Virtual Data” concept
- **Particle Physics Data Grid (DOE Science)**
  - DG applications for HENP
- **Earth System Grid (DOE Science)**
  - DG technologies, climate applications
- **Information Power Grid (NASA)**
  - DG applications

Particle Physics Data Grid

Large Hadron Collider,
CERN, Switzerland



CMS

~PBytes/sec

Online System

~100 MBytes/sec

1 TIPS is approximately 25,000 SpecInt95 equivalents

There is a "bunch crossing" every 25 nsecs.

There are 100 "triggers" per second

Each triggered event is ~1 MByte in size

Offline Processor Farm
~20 TIPS

~100 MBytes/sec

Tier 0

CERN Computer Centre

HPSS

~622 Mbits/sec
or Air Freight (deprecated)

Tier 1

France Regional Centre

Germany Regional Centre

Italy Regional Centre

FermiLab ~4 TIPS

~622 Mbits/sec

Tier 2

Caltech
~1 TIPS

Tier2 Centre
~1 TIPS

Centre
TIPS

Centre
1 TIPS

Centre
1 TIPS

~622 Mbits/sec

Institute
~0.25TIPS

tute

stitute

Institute

Physics data cache

~1 MBytes/sec

Tier 4

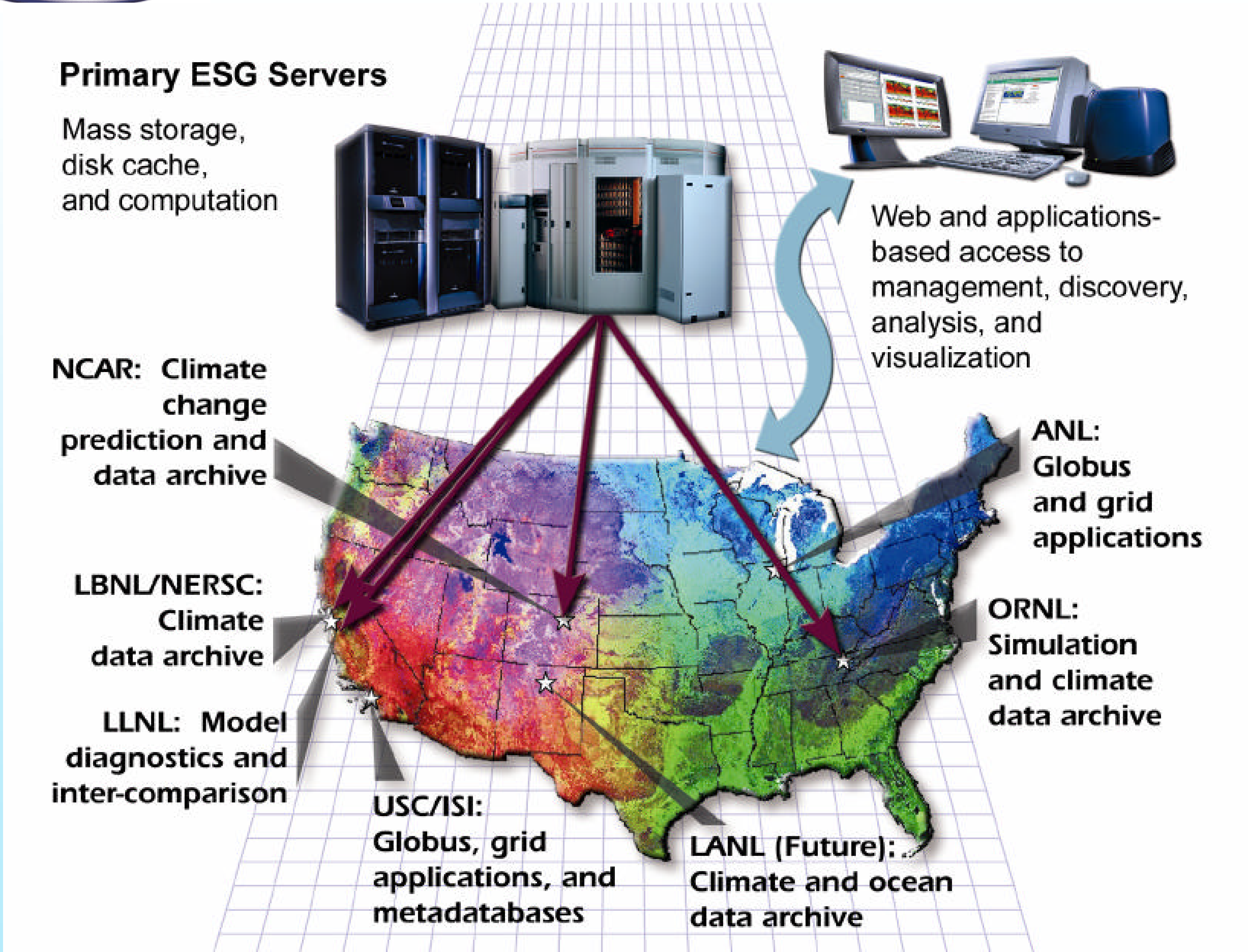
Physicist workstations

Physicists work on analysis "channels".

Each institute will have ~10 physicists working on one or more channels; data for these channels should be cached by the institute server

Image courtesy Harvey Newman, Caltech

Earth System Grid


Primary ESG Servers
Mass storage,
disk cache,
and computation
Web and applications-based access to management, discovery, analysis, and visualization
NCAR: Climate change prediction and data archive
ANL: Globus and grid applications
LBNL/NERSC: Climate data archive
ORNL: Simulation and climate data archive
LLNL: Model diagnostics and inter-comparison
USC/ISI: Globus, grid applications, and metadatabases
LANL (Future): Climate and ocean data archive

Security Implications of Grid Computing (1)

- **Need to allow access to trusted sources, but how do you determine trust in a dynamic community of thousands (or more) in different organizations?**
- **Need to allow Web services on port 80 (HTTP) or port 443 (SSL, HTTPS) through the firewall**
  - Application level firewalls
- **Companies such as IBM, HP, and Microsoft offer commercial grid software and services, but typically only for Intragrids (inside organizations) where security can be managed coherently**
- **The more interesting security issue is the virtual organization or Intergrid**
  - Unsolved problem, because current solutions create Federations of Enterprises based on pair-wise trust agreements; these don’t scale

Security Implications of Grid Computing (2)

- **Today Globus Toolkit uses Public Key Infrastructure for both authentication and authorization**
- **Some experts advocate using PKI only for authentication (based on a certificate authority)**
- **Use directory services for authorization (probably LDAP) with communication through Security Assertion Markup Language (SAML)**
  - Shibboleth is a reference implementation http://shibboleth.internet2.edu
- **SAML is a web-based language (over HTTP) that allows three kinds of messages:**
  - Attribute assertions
  - Authentication assertions
  - Authorization assertions
- **For some transactions we need to add privacy**
  - How to anonymize identity, attributes, actions, and personal data?
  - Being researched as part of the DARPA Total Information Awareness project

Why should we care about privacy?

- **History has shown that available information can be abused to persecute individuals with differing beliefs**
  - Nazi Germany
  - Stalinist Russia
  - Maoist China
  - Iraq under Hussein
- **Even in the US**
  - Exile of Nisei from coastal California in WW2
  - McCarthy anti-Communist hearings
  - CIA domestic spying (Church committee hearings of 1973)
- **Laws explicitly safeguard some information privacy**
  - Gramm-Leach-Bliley Act covers privacy of financial records
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers privacy of medical records
  - European Union Directive 95/46 covers protection of personal data

Example of Middleware: Web Services

- Architecture and program interfaces that enable application-to-application communication
- Run primarily on top of http (or https) web protocols
- Allow aggregation of functions provided by heterogeneous software modules, including legacy apps
- Allow changes to underlying components without manual reprogramming
- Allow seamless extension of functions and services

Web Services are Emerging Standards for eCommerce

- XML (Extensible Markup Language) defines a universal way of representing any data; allows exchange of data between any applications regardless of operating system, language, hardware, user device
- SOAP (Simple Object Access Protocol) defines universal Web service requests using XML messages, making process integration simple
- WSDL (Web Services Definition Language) specifies information needed for integration among applications
- UDDI (Universal Description, Discovery, and Integration) is a Web service that allows users and applications to locate other Web services

Security in Web Services is Just Being Developed

- **HTTPS/SSL for secure point-to-point communication with known trusted parties, but**
  - no authorization, auditing, non-repudiation
  - not end-to-end, stops at HTTPS server
  - no digital signature verification through to the data base
- **WS-Security: message level security protocol**
  - persists end-to-end
  - interoperable with web services such as SOAP, SSL, Kerberos, PKI, SAML, etc.
  - http://www-106.ibm.com/developerworks/library/ws-secmap/
- **Managing trust issues is still a challenge**

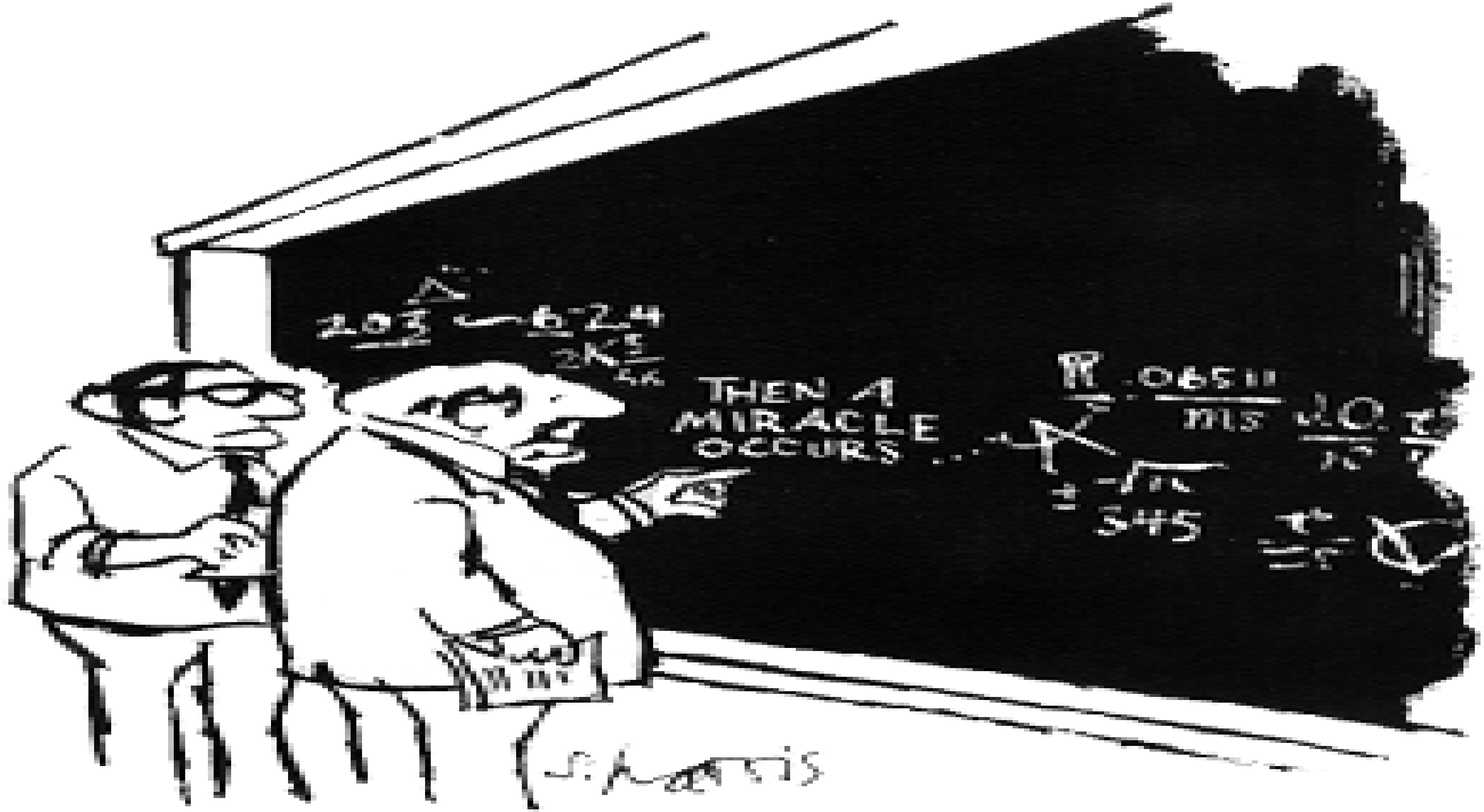
Emerging Issue of Role-Based Security

- **Role based security: Each of us assumes different roles with different security requirement. One individual may act as:**
  - Manager signing timecards or authorizing procurement
  - Researcher working on data with foreign collaborators
  - Individual buying books from Amazon.com at lunch hour
- **How to handle these different roles using common equipment (PC, network)?**
- **Alternative is separate networks and equipment for each role that requires a different levels of security or access - cumbersome and impractical**

Summary

- Future computing environment is likely to be more enterprise-critical, distributed, and dynamic than today
- Maintaining security will be challenging
- New security inventions will likely be needed

Then a Miracle Occurs



"I think you should be more explicit here in step two."

For Further Information

Please contact us at:

nco@itrd.gov

Or visit us on the Web:

www.itrd.gov